Social Security Number Protection Task Force

Report to the Illinois General Assembly, Governor Pat Quinn,
and Secretary of State Jesse White
December 31, 2012

CONTENTS

TASK FORCE BACKGROUND

The Social Security Number (SSN) remains the key piece of sensitive personally identifiable information that identity thieves use to commit fraud. The SSN was intended to be used solely to distribute Social Security benefits, but in the years since its inception in 1935, it has been also used as a unique identification number. The SSN is therefore not only tied to an individual's credit report, financial records, and Social Security earnings with the federal government, but is also present in employment, educational, health, insurance, and criminal records. The wide dissemination of SSNs increases the likelihood that the numbers can be accessed and subsequently used for fraudulent purposes.

Consumers are therefore encouraged to limit their exposure to identity theft by protecting their SSNs. Businesses are also encouraged to do their part by taking necessary steps to limit the collection of SSNs, protect SSNs in their possession, and dispose of documents containing SSNs in a manner that renders them unusable. Local and state government agencies also have a role in protecting SSNs they maintain and reducing their continued widespread dissemination. Government agencies have the larger task of maintaining a system of open records for the public, while taking measures to reduce the amount of sensitive personally identifiable information in those records.

RECENT PRIVACY DEVELOPMENT

In early 2012 the White House issued a report entitled *Consumer Data Privacy In a Networked World: A Framework For Protecting Privacy And Promoting Innovation In the Global Digital Economy* ("Privacy Report"). This Privacy Report listed seven core principles that business stakeholders will be encouraged to implement so that consumers may have increased trust that companies are effectively addressing privacy concerns in our increasingly networked society. The seven principles were created from what is now known as the Consumer Privacy Bill of Rights. These principles are: (1) Individual Control – Consumers have the right to exercise control over what personal data companies collect from them and how they use it; (2) Transparency – Consumers have a right to easily understandable and accessible information about privacy and security practices; (3) Respect for Context – Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data; (4) Security – Consumers have the right to secure and responsible handling of personal data; (5) Access and Accuracy – Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate; (6) Focused Collection – Consumers have a right to reasonable limits on the personal data that companies collect and retain; and (7) Accountability – Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights. These principles were based largely from the universally accepted framework for privacy protections, the Fair Information Practice Principles (FIPPs) of the Organization for Economic Co-operation and Development ("OECD"), Department of Homeland Security Privacy Policy ("DHS"), and the Asia-Pacific Economic Cooperation Principals ("APEC"). This newly created Consumer Privacy Bill of Rights applies to all commercial uses of personal data, including data which may be linked directly to a specific individual, thus the principles aid in protecting SSNs and limiting their widespread dissemination

and potential misuse. With the advent of mobile payments and smartphone applications the need for commercial guidance over safeguarding consumer information has never been greater.

MEMBERSHIP OF THE TASK FORCE

- Two members representing the House of Representatives, appointed by the Speaker of the House – **Representative Sara Feigenholtz, Representative Ann Williams**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – **Representative Sandra Pihos, Representative Kay Hatcher**
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jeffrey Schoenberg, Senator Jacqueline Collins**
- Two members representing the Senate, appointed by the Minority Leader of the Senate – **Senator Chris Lauzen, Senator Dan Duffy**
- One member representing the Office of the Attorney General – **Deborah Hagan, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**
- One member representing the Office of the Governor – **Jay Stewart**
- One member representing the Department of Natural Resources – **John Pohlman "J.J."**
- One member representing the Department of Healthcare and Family Services – **Tamara Hoffman**
- One member representing the Department of Revenue – **George Logan**
- One member representing the Department of State Police – **Greg Muller**
- One member representing the Department of Employment Security – **Joseph Mueller**
- One member representing the Illinois Courts – **James Morphew**
- One member representing the Department on Aging – **Patricia Carter**
- One member representing Central Management Services – **Robert Morgan**
- One member appointed by the Executive Director of the Board of Higher Education – **Don Sevener**
- One member appointed by the Secretary of Human Services – **Solomon Oriaikhi**
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – **Alissa Camp**
- One member representing school administrators, appointed by the State Superintendent of Education – **Sara Boucek**

PART I: PROTECTION OF SSNS IN THE PUBLIC RECORD

The first statutory requirement of the Social Security Number Protection Task Force Act is to examine the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN.

Identity Protection Act

One way to limit the unauthorized disclosure of SSNs is to limit their collection in the first place. If fewer entities collect and use SSNs, fewer entities are capable of disclosing those numbers improperly.

The Identity Protection Act (5 ILCS 179/1 *et seq*.) prohibits certain collections, uses and disclosures of an individual's SSN by any person, or State or local government agencies. Specifically, the Act, with several exceptions, prohibits a person, or State or local government agency, from: collecting, using, or disclosing a SSN unless (1) required to do so under state or federal law or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the agency's duties and responsibilities; (2) the need and purpose for the SSN is documented before the request; and (3) the SSN collected is relevant to the documented need and purpose. The need and purpose for the collection and use of SSNs must be documented in a written Identity-Protection Policy.

Each local government agency must file a written copy of its policy with the governing board of the unit of local government within 30 days after approval of the policy. Under Section 37(b), "each State agency must provide a copy of its identity-protection policy to the Social Security Number Protection Task Force within 30 days after the approval of the policy." State government agencies were reminded of this requirement on August 24, 2011. Policies can be submitted to the Task Force by mailing a copy to:

Illinois Attorney General
Social Security Number Protection Task Force
c/o: AAG Matthew W. Van Hise
500 S. Second Street
Springfield, IL. 62706

As part of the implementation of the policies, local and state agencies will require that all employees identified as having access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. Training should include instructions on the proper handling of information that contains SSNs from the time of collection through the destruction of the information.

Identity-Protection Policies were to have been implemented within 12 months of the date of approval and a copy was to have been sent to the Social Security Number Protection Task Force no later than June 1, 2012. Courtesy reminders will be made by the Task Force beginning January 2013, to all entities that have failed to meet the 2012 deadline for implementation.

<u>Consumer Fraud and Deceptive Business Practices Act ("Consumer Fraud Act")</u>
Following the guidance provided by the Identity Protection Act (5 ILCS 179/1 *et seq.*), which limits the purposes for which any person, State or local governmental agency may collect, use and disclose an individuals' SSN; the Illinois Consumer Fraud Act was amended by P.A. 97-139 and as of January 1, 2012 includes further guidance over the use of SSNs.

P.A. 97-239 amended Section 2RR of the Consumer Fraud Act (815 ILCS 505/2RR) to add wristbands and the outsides of files to the list of prohibited places for SSN display. These are in addition to the previously existing prohibitions on: publically posting or publically displaying an individual's SSN; printing an individual's SSN on any card; requiring an individual to transmit his or her SSN over the Internet, unless the connection is secure or the SSN is encrypted; requiring an individual to use his or her SSN to access an Internet web site, unless a password or

unique personal identification number or other means of authentication is required to access the site; and lastly printing of an individual's SSN on any materials that are mailed to the individual, unless State or federal law requires otherwise.

Section 2RR of the Consumer Fraud Act also currently provides the following as to SSNs: (1) A person or entity that provides an insurance card must print on the card an identification number unique to the holder of the card in the format prescribed by Section 15 of the Uniform Prescription Drug Information Card Act; and (2) SSNs may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the SSN; however, the SSN may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope or visible without the envelope having been opened.

An exception to the above mentioned amendment was included for persons that used, prior to July 1, 2005, an individual's SSN in a manner inconsistent with these requirements if: (1) the use of the SSN is continuous, and the use has not stopped for any reason; and (2) the individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her SSN in a matter dictated per the recent amendment.

An important point to mention is that the recent amendment does not apply to the collection, use, or release of a social security number as required by State or federal law, or the use of a SSN for internal verification or administrative purposes. Additionally, this amendment does not apply to the collection, use, or release of a SSN by the State, a subdivision of the State, or an individual in the employ of the State or a subdivision of the State in connection with his or her official duties; nor does it apply to documents that are recorded or required to be open to the public under State or federal law, applicable case law, Supreme Court Rules, or the Constitution of the State of Illinois.

Lastly, the amendment provides: (1) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, any person who complies with the federal law shall be deemed to be in compliance with these amendments; and (2) A person may not encode or embed a SSN in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the SSN.

Any person who violates these recent amendments commits an unlawful practice within the meaning of the Consumer Fraud Act.

(2012 Amendment – Appendix A)

Children and Family Services Act

In examining the procedures used by the State to protect individuals against the unauthorized disclosure of their SSN, it was important to ensure that all individuals, especially those easily

overlooked by ordinary safeguards, are protected by statutory assurances such as those found in the Children and Family Services Act.

The Children and Family Services Act (20 ILCS 505/1 *et seq.*) was amended in 2010 to require that the Department of Children and Family Services ("DCFS") conduct annual credit history checks to determine the financial history of children placed under its guardianship.

The amendment dictates that when a ward of the state turns 12 years old, DCFS shall conduct a credit check on behalf of the ward to determine if financial exploitation of the child's personal information has occurred. This check is to occur annually and throughout the duration of the guardianship until guardianship is terminated pursuant to the Juvenile Court Act of 1987. In the event that exploitation appears to have occurred, DCFS shall notify the proper law enforcement agency, including local State's Attorney or the Illinois Attorney General.

Currently, the Illinois Attorney General's Office operates an Identity Theft Unit, which was established in February of 2006. Upon becoming aware of the DCFS requirement of conducting annual credit history checks on wards 12 years and older, the ID Theft Unit has worked in conjunction with DCFS to assist with resolving erroneous and fraudulent discrepancies pertaining to the foster youths.

In many of these situations the youth's SSN has been used in an unauthorized manner to facilitate financial exploitation of the child. By amending this Act, additional procedures and safeguards have been created to protect SSN's of a class of Illinois citizens that are easily overlooked due to their status as minors. To date, since 2010, the Illinois Attorney General's Office has received over 217 identity theft complaints for DCFS minors, some as young as 2 years of age.

(2010 Amendment – Appendix B)

PART II: SSNs AS INTERNAL IDENTIFIERS

The second requirement of the Task Force is to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs for identification and record-keeping purposes by State and local governments. State and local government agencies continue to internally assess the collection and use of SSNs. Such an assessment was critical in drafting Identity Protection Policies. Ongoing assessments will be necessary in carrying out these policies as implemented.

PERSONAL INFORMATION PROTECTION ACT

Public Act 97-0483, enacted August 22, 2011, amends the Personal Information Protection Act (PIPA). As of January 1, 2012 the following amendments to PIPA became effective.

PIPA requires entities that suffer security breaches of personal information to notify affected individuals of the breach without unreasonable delay. Notification in the event of a breach allows affected individuals to take steps to protect themselves against identity theft or other financial fraud. A breach is defined as the unauthorized acquisition of computerized data that

compromises the security, confidentiality, or integrity of personal information. Personal information is an individual's name combined with SSN, driver's license number, or financial account number. It is important for Task Force members to be aware of the requirements of PIPA because the Act applies to state agencies that collect this data. In addition, although the breach notification is limited to computerized data for most entities, notification must go out from state agencies when there has been a breach of *written* material as well as computerized data.

As amended, PIPA now requires entities to include specific information in the breach notification letter. The disclosure notification to an Illinois resident shall include, but need not be limited to:

(i) the toll-free numbers and addresses for consumer reporting agencies,
(ii) the toll-free number, address, and website address for the Federal Trade Commission, and
(iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

The amendment also clarifies the responsibilities of data collectors that maintain personal information, but do not own or license such information. Under existing law, entities that maintain the data that suffer breaches must notify the data owner immediately upon discovery of the breach. The amendment adds the following requirement:

> In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

Lastly, PIPA is amended by adding a new section for the proper disposal of materials containing personal information. Proper disposal of material that contains personal information is a necessary step in protecting individuals against identity theft and financial fraud. Incidents of identity theft occur when "dumpster divers" find troves of valuable personal information in publicly available garbage bins. In addition, personal information left on computers and other electronic media can be accessed and misused with relative ease.

There are several federal requirements for proper disposal of materials containing personal information. The Safeguards Rule, a federal regulation that implements the Gramm-Leach-Bliley Act, obligates a financial institution to protect the security and confidentiality of customers' nonpublic personal information by implementing and maintaining a written information security program that includes procedures for proper disposal. The Disposal Rule, a federal regulation that implements the Fair Credit Reporting Act, requires entities that possess or

maintain consumer reports, or records derived from a consumer report, to properly dispose of those reports by taking reasonable measures to protect against unauthorized access. No such similar law existed in Illinois until now, with the addition of Section 40 to PIPA, which adds proper disposal guidelines for those holding materials containing personal information.

Any person who violates this amendment pertaining to disposal procedures is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section.

(2012 Amendment – Appendix C)

TASK FORCE APPOINTMENTS & UPDATES

Ann Williams, State Representative, was appointed by the Speaker of the House.
John Pohlman "J.J.", Director – Office of Administration, was appointed by the Director of Natural Resources.
Tamara Hoffman, Chief of Staff, was appointed by the Director of Healthcare and Family Services.
Greg Muller, Department Director of Administration, was appointed by the Director of the Illinois State Police.
Patricia Carter, Chief Financial Officer, was appointed by the Director of the Department of Aging.
Don Sevener, Department Director of External Relations, was appointed by the Executive Director of the Boards of Higher Education.
Solomon Oriaikhi, Director – Office of Fiscal Services, was appointed by the Secretary of Human Services.
Alissa Camp, Chief Legal Counsel, was appointed by the Illinois Comptroller.

CONCLUSION

Identity-Protection Policies at local and State government agencies throughout Illinois have been implemented per the requirements of the Identity Protection Act. Additionally, recent amendments to the Consumer Fraud and Deceptive Business Practices Act and Children and Family Services Act have sought to further limit the posting, displaying, and transmitting of an individual's SSN; as well as help protect wards of the state from financial exploitation. Furthermore, the Personal Information Protection Act now specifies that entities follow certain reporting requirements in the event of a data breach; clarifies how data collectors who do not own or license the information they collect and store maintain personal information; and details how to properly dispose of materials containing personal information. The Task Force membership will continue to work together with all stakeholders to identify the best ways to protect SSNs in public records and limit the use of SSNs as internal identifiers.

APPENDIX A

(815 ILCS 505/2RR) Consumer Fraud and Deceptive Business Practices Act

Sec. 2RR. Use of Social Security numbers.
(a) Except as otherwise provided in this Section, a person may not do any of the following:
(1) Publicly post or publicly display in any manner an individual's social security number. As used in this Section, "publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.
(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity, or on a wristband or on the outside of any file associated with the products or services provided by the person or entity; however, a person or entity that provides an insurance card must print on the card an identification number unique to the holder of the card in the format prescribed by Section 15 of the Uniform Prescription Drug Information Card Act.
(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.
(4) Require an individual to use his or her social security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.
(5) Print an individual's social security number on any materials that are mailed to the individual, unless State or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope or visible without the envelope having been opened.
(b) A person that used, before July 1, 2005, an individual's social security number in a manner inconsistent with subsection (a) may continue using that individual's social security number in the same manner on or after July 1, 2005 if all of the following conditions are met:
(1) The use of the social security number is continuous. If the use is stopped for any reason, subsection (a) shall apply.
(2) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or

her social security number in a manner prohibited by subsection (a).

A written request by an individual to stop the use of his or her social security number in a manner prohibited by subsection (a) shall be implemented within 30 days of the receipt of the request. There shall be no fee or charge for implementing the request. A person shall not deny services to an individual because the individual makes such a written request.

(c) This Section does not apply to the collection, use, or release of a social security number as required by State or federal law or the use of a social security number for internal verification or administrative purposes. This Section does not apply to the collection, use, or release of a social security number by the State, a subdivision of the State, or an individual in the employ of the State or a subdivision of the State in connection with his or her official duties.

(d) This Section does not apply to documents that are recorded or required to be open to the public under State or federal law, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.

(e) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, any person who complies with the federal law shall be deemed to be in compliance with this Section.

(f) A person may not encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this Section.

(g) Any person who violates this Section commits an unlawful practice within the meaning of this Act.

(Source: P.A. 97-139, eff. 1-1-12.)

APPENDIX B

(20 ILCS 505/5) Children and Family Services Act

> (x) The Department shall conduct annual credit history checks to determine the financial history of children placed under its guardianship pursuant to the Juvenile Court Act of 1987. The Department shall conduct such credit checks starting when a ward turns 12 years old and each year thereafter for the duration of the guardianship as terminated pursuant to the Juvenile Court Act of 1987. The Department shall determine if financial exploitation of the child's personal information has occurred. If financial exploitation appears to have taken place or is presently ongoing, the Department shall notify the proper law enforcement agency, the proper State's Attorney, or the Attorney General.

APPENDIX C

(815 ILCS 530/5) Personal Information Protection Act

Sec. 5. Definitions. In this Act:
"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.
"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.
"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
(1) Social Security number.
(2) Driver's license number or State identification card number.
(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.
(Source: P.A. 97-483, eff. 1-1-12.)

(815 ILCS 530/10) Personal Information Protection Act

Sec. 10. Notice of Breach.
(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the

toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is
consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector
demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies

subject persons in accordance with its policies in the event of a breach of the security of the system data.
(Source: P.A. 97-483, eff. 1-1-12.)

(815 ILCS 530/12) Personal Information Protection Act

Sec. 12. Notice of breach; State agency.
(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.
(a-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the State agency with a written request for the delay. However, the State agency must notify the Illinois resident as soon as notification will no longer interfere with the investigation.
(b) For purposes of this Section, notice to residents may be provided by one of the following methods:
(1) written notice;
(2) electronic notice, if the notice provided is
consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
(3) substitute notice, if the State agency
demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the State agency has an email address for the subject persons; (ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and (iii) notification to major statewide media.
(c) Notwithstanding subsection (b), a State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing

requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.
(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.
(Source: P.A. 97-483, eff. 1-1-12.)

(815 ILCS 530/40) Personal Information Protection Act

Sec. 40. Disposal of materials containing personal information; Attorney General.
(a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.
(b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:
(1) Paper documents containing personal information
may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.
(2) Electronic media and other non-paper media
containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.
(c) Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.
(d) Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed $50,000 for each instance of improper disposal of

materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

(f) A financial institution under 15 U.S.C. 6801 et. seq. or any person subject to 15 U.S.C. 1681w is exempt from this Section.

(Source: P.A. 97-483, eff. 1-1-12.)